Discrete Mathematics 68 (1988) 45–57
North-Holland

HADAMARD MATRICES OF THE WILLIAMSON TYPE OF ORDER $4 \cdot m$, $m = p \cdot q$ AN EXHAUSTIVE SEARCH FOR $m = 33$

Christos KOUKOUVINOS and Stratis KOUNIAS
Department of Mathematics, University of Thessaloniki, Thessaloniki, Greece 54006

Received 15 October 1986

All circulant and symmetric $(1, -1)$ matrices A, B, C, D of order $m = 33$ such that $A^2 + B^2 + C^2 + D^2 = 4mI_m$ are constructed.

These are called matrices of the Williamson type.

An algorithm is given reducing considerably the required computational time and suitable when m is not a prime.

It is established that there are four non-equivalent Hadamard matrices of the Williamson type of order $4 \cdot 33$.

1. Introduction

An Hadamard matrix is a square matrix of ones and minus ones whose row (and hence column) vectors are orthogonal.

The order n of an Hadamard matrix is necessarily 1, 2 or $4m$, with m a positive integer. For more details for their construction see [5, 6, 12]. Since we can easily construct an Hadamard matrix of order $2n$, from one of order n, the interest lies in the case $n = 4m$ where m is odd.

In particular if a Baumert–Hall array of order t and Williamson matrices of order m are known, then there exists an Hadamard matrix of order $4mt$. Note that Baumert–Hall arrays of order t are known for many values of t, see [1; 7, p. 145; 10 and 12, p. 360]. Hence the potential number of solutions of order $4mt$ is increased by increasing the number of solutions of order m and/or t.

In this paper we are interested in constructing matrices of the Williamson type of order $4 \cdot m$, m odd, $m = p \cdot q$, $p, q > 1$.

The quadruple of $(1, -1)$ matrices A, B, C, D of order m is of the Williamson type if:

(i) $MN^{\mathrm{T}} = NM^{\mathrm{T}}$, $M, N \in \{A, B, C, D\}$

(ii) $AA^{\mathrm{T}} + BB^{\mathrm{T}} + CC^{\mathrm{T}} + DD^{\mathrm{T}} = 4mI_m$.

Such matrices have been constructed for many values of m, see [9 and 12, pp. 388–389].

Infinite classes of Hadamard matrices of the Williamson type have been constructed by Turyn [11] and Whiteman [13]. Originally Williamson [14]

considered circulant and symmetric A, B, C, D and constructed them for $m \leq 21$, $m = 25, 37, 43$.

Note that neither the circulant nor symmetric are necessary properties in order to satisfy (i) and (ii).

From now on by Williamson type we mean a quadruple of circulant and symmetric $(1, -1)$-matrices satisfying (i) and (ii).

Baumert, Golomb and Hall [3] constructed an Hadamard matrix of the Williamson type for $m = 23$, Baumert and Hall [4] gave all solutions for $3 \leq m \leq 23$ and some solutions for $m = 25, 27, 37, 43$ and Baumert [2] gave one solution for $m = 29$. Sawade [8] did an exhaustive search for $m = 25, 27$. Also Yamada [15] considered a restricted class of the Williamson type and gave a new one for $m = 37$.

The exhaustive search for Williamson type matrices for $m \geq 29$, however, turns out to be much more difficult because of the formidable computational time.

In this paper we give an algorithm suitable when m is not a prime. With this algorithm the computational time is reduced considerably. When $n = 4 \cdot m$, m odd, $m = p \cdot q$ with $p, q > 1$ our algorithm is implemented by first finding all solutions mod p, then mod q and then merging them. This gives a considerable reduction in computer time and we demonstrate our method in Section 4 when $m = 33$. We also give an example in Section 3 when $m = 15$, in this case applying our method the exhaustive search is reduced to a few cases and is done by hand.

Note that for $m = 33$ we cannot obtain solutions applying Turyn's method [11] which requires $2m - 1 = q \equiv 1 \pmod 4$ to be prime power.

In [9] Seberry constructed A, B, C, D of order $m = 33$, satisfying (i) and (ii), where A is skew-symmetric and B, C, D are symmetric block-circulant matrices.

The reduction in computer time is considerable if $p \neq q$. When $p = q$ we achieve also a reduction by finding all solutions mod p and then construct the quadruple A, B, C, D.

If we have a quadruple of Williamson type matrices of order $n = 4m$, $A = (a_0, a_1, \ldots, a_{m-1})$, $B = (b_0, b_1, \ldots, b_{m-1})$, $C = (c_0, c_1, \ldots, c_{m-1})$, $D = (d_0, d_1, \ldots, d_{m-1})$, then applying the transformation $j \to j \cdot s \pmod m$, $(s, m) = 1$, we obtain another quadruple of Williamson type matrices. These quadruples are called equivalent and we need to know only one quadruple from each equivalent class.

In each equivalent class there are at most $\frac{1}{2}\varphi(m)$ such quadruples where $\varphi(m)$ is the number of integers $s : (s, m) = 1$, $0 < s < m$. This is because some quadruples may be transformed into themselves and the transformations $j \to j \cdot s \pmod m$ and $j \to j(m - s) \pmod m$ are identical due to the symmetry of A, B, C, D.

There are four different representations of $132 = 4 \cdot 33$ as the sum of four odd squares, i.e.,

(i) $11^2 + 3^2 + 1^2 + 1^2$,

(ii) $9^2+7^2+1^2+1^2$,

(iii) $9^2+5^2+5^2+1^2$,

(iv) $7^2+7^2+5^2+3^2$,

With the application of our algorithm we found that (i) gives no solution, (ii) gives one solution, (iii) gives two non-equivalent solutions and (iv) gives one solution. These solutions, up to equivalence, are given in the Appendix.

Hence there are altogether four non-equivalent Williamson type matrices of order $4 \cdot 33$.

We have also applied our algorithm for $m = 9, 15, 21, 25, 27$ where an exhaustive search has been done before, [4, 8] and our results agree with the existing ones.

In what follows we prove some results needed for our algorithm. It is known that if the Williamson equation is satisfied on the commutative (cyclic) group, then it is satisfied on a subgroup. This is essentially shown in Theorem 1 of Section 2, but in a context suitable for our purposes. In Section 2, Theorem 2, we prove a result similar to Williamson's which is useful for our algorithm.

2. The method

In this section we give the necessary tools needed for our algorithm.

We want to construct the circulant and symmetric $(1, -1)$-matrices:

$$A = (a_0, a_1, \ldots, a_{m-1}), \qquad B = (b_0, b_1, \ldots, b_{m-1}),$$
$$C = (c_0, c_1, \ldots, c_{m-1}), \qquad D = (d_0, d_1, \ldots, d_{m-1}),$$

such that

$$A^2 + B^2 + C^2 + D^2 = 4mI_m. \tag{1}$$

From the symmetry requirement we have

$$v_i = v_{m-i}, \quad i = 1, 2, \ldots, \tfrac{1}{2}(m-1), \quad v_i \in \{a_i, b_i, c_i, d_i\}.$$

Let $G_q^{\mathrm{T}} = (I_p, I_p, \ldots, I_p)$ be a $p \times p \cdot q$ matrix, i.e., the unit matrix I_p of order p is repeated q times.

Theorem 1. *If*

(i) $m = p \cdot q$, $p, q > 1$,

(ii) $V = (v_0, v_1, \ldots, v_{m-1})$ *is circulant of order* m,

then (i) $G_q^{\mathrm{T}} \cdot V = U \cdot G_q^{\mathrm{T}}$, *where* $U = (u_0, u_1, \ldots, u_{p-1})$ *is circulant of order* p *with*

$$u_j = \sum_{\substack{i \equiv j \pmod p \\ i < m}} v_i, \quad j = 0, 1, \ldots, p-1,$$

(ii) *U is symmetric if V is symmetric.*

Proof. (i) If $Q_m = (0, 1, 0, \ldots, 0)$ is circulant of order m, then $Q_m^m = I_m$, $(Q_m^i)^T = Q_m^{m-i}$, $i = 1, 2, \ldots, m-1$ and $G_q^T Q_m = Q_p G_q^T$. Hence $G_q^T Q_m^i = Q_p^i G_q^T$ and

$$G_q^T V = G_q^T\Big(\sum_{i=0}^{m-1} v_i Q_m^i\Big) = \sum_{i=0}^{m-1} v_i G_q^T Q_m^i = \Big(\sum_{i=0}^{m-1} v_i Q_p^i\Big) G_q^T.$$

But

$$\sum_{i=0}^{m-1} v_i Q_p^i = \sum_{j=0}^{p-1}\Big(\sum_{\substack{i\equiv j \,(\mathrm{mod}\, p)\\ i<m}} v_i\Big) Q_p^j = \sum_{j=0}^{p-1} u_j Q_p^j = (u_0, u_1, \ldots, u_{p-1}) = U,$$

because $Q_p^i = Q_p^j$ $\forall i \equiv j \pmod p$.

(ii) If V is symmetric, then

$$u_j = \sum_{\substack{i\equiv j \,(\mathrm{mod}\, p)\\ i<m}} v_i = \sum_{\substack{i\equiv j \,(\mathrm{mod}\, p)\\ i<m}} v_{m-i}$$

$$= \sum_{\substack{s\equiv (p-j) \,(\mathrm{mod}\, p)\\ s<m}} v_s = u_{p-j}, \quad j = 1, 2, \ldots, \tfrac{1}{2}(p-1). \quad \square$$

Now multiplying on the left A, B, C, D by G_q^T we obtain:

$$G_q^T A = X_p G_q^T, \qquad G_q^T B = Y_p G_q^T, \qquad G_q^T C = Z_p G_q^T, \qquad G_q^T D = W_p G_q^T,$$

where

$$\begin{aligned} X_p &= (x_0, x_1, \ldots, x_{p-1}), && \text{with } x_j = \sum_i a_i,\\ Y_p &= (y_0, y_1, \ldots, y_{p-1}), && \text{with } y_j = \sum_i b_i,\\ Z_p &= (z_0, z_1, \ldots, z_{p-1}), && \text{with } z_j = \sum_i c_i,\\ W_p &= (w_0, w_1, \ldots, w_{p-1}), && \text{with } w_j = \sum_i d_i, \end{aligned} \tag{2}$$

and the summations are over all $i \equiv j \pmod p$, $i < m$.

If we multiply both members of (1), on the left by G_q^T and on the right by G_q we obtain in the symmetric case:

$$X_p^2 + Y_p^2 + Z_p^2 + W_p^2 = 4mI_p. \tag{3}$$

Of course we do not know A, B, C, D so we do not know X_p, Y_p, Z_p, W_p. However it is easier to find X_p, Y_p, Z_p, W_p satisfying (3) than A, B, C, D because p is much smaller than m. Now to construct X_p, Y_p, Z_p, W_p note that:

Theorem 2. *If* (i) A, B, C, D *are circulant and symmetric* $(+1, -1)$*-matrices satisfying* (1) *with row (and hence column) sums* a, b, c, d,

(ii) X_p, Y_p, Z_p, W_p *are as defined in* (2),

then

$$\text{(i)}\quad \sum_{j=0}^{p-1} x_j = a, \quad \sum_{j=0}^{p-1} y_j = b, \quad \sum_{j=0}^{p-1} z_j = c, \quad \sum_{j=0}^{p-1} w_j = d,$$
$$a^2+b^2+c^2+d^2 = 4m, \quad -q \leqslant x_j, y_j, z_j, w_j \leqslant q, \quad x_j, y_j, z_j, w_j \text{ odd},$$
$$x_j = x_{p-j}, \quad y_j = y_{p-j}, \quad z_j = z_{p-j}, \quad w_j = w_{p-j}, \quad j = 1, 2, \ldots, \tfrac{1}{2}(p-1), \tag{4}$$

(ii) *If moreover* $a_0+b_0+c_0+d_0 = 0, \pm 4$, *then*

$$(x_0+y_0+z_0+w_0)-(a_0+b_0+c_0+d_0) = \begin{cases} 0 \pmod 8, & \text{if } q \equiv 1 \pmod 4, \\ 4 \pmod 8, & \text{if } q \equiv 3 \pmod 4, \end{cases} \tag{5}$$
$$x_j+y_j+z_j+w_j \equiv 2 \pmod 4, \quad j = 1, 2, \ldots, \tfrac{1}{2}(p-1).$$

Proof. (i) From (2) we have

$$\sum_{j=0}^{p-1} \lambda_j = \sum_{j=0}^{p-1} \Bigg(\sum_{\substack{i \equiv j \pmod p \\ i<m}} a_i \Bigg) = \sum_{i=0}^{m-1} a_i = a.$$

From the symmetry of A and (2) we have

$$x_j = x_{p-j}, \quad j = 1, 2, \ldots, \tfrac{1}{2}(p-1).$$

Since $a_i = \pm 1$ and both p, q are odd then x_j being the sum of an odd number (q) of ± 1 is odd and $-q \leqslant x_j \leqslant q$. Similarly for y_j, z_j, w_j.

(ii) Williamson [14] (see also [5, p. 219] or [12, p. 384]) proved that if $a_0 = b_0 = c_0 = d_0$, then $a_j+b_j+c_j+d_j = \pm 2$.

From (2) we have:

$$(x_0+y_0+z_0+w_0)-(a_0+b_0+c_0+d_0) = 2\sum_i (a_i+b_i+c_i+d_i),$$

the summation is for, $1 < i < \frac{1}{2}(m-1)$, $i \equiv 0 \pmod p$. If $q \equiv 1 \pmod 4$ we are summing up $\frac{1}{2}(q-1) \equiv 0 \pmod 2$ terms, each equal to ± 2, hence

$$(x_0+y_0+z_0+w_0)-(a_0+b_0+c_0+d_0) \equiv 0 \pmod 8.$$

If $q \equiv 3 \pmod 4$ we are summing up $\frac{1}{2}(q-1) \equiv 1 \pmod 2$ terms, each equal to ± 2, hence

$$(x_0+y_0+z_0+w_0)-(a_0+b_0+c_0+d_0) \equiv 4 \pmod 8.$$

Also

$$x_j+y_j+z_j+w_j = \sum_{\substack{i \equiv j \pmod p \\ i<m}} (a_i+b_i+c_i+d_i),$$

in the summation sign are q (odd) terms each equal to ± 2, hence

$$x_j+y_j+z_j+w_j \equiv 2 \pmod 4, \quad j = 1, 2, \ldots, \tfrac{1}{2}(p-1).$$

The result of Williamson is still valid if $a_0+b_0+c_0+d_0 = 0$ because if say $c_0 = d_0 = -1$, then consider A, B, $-C$, $-D$, where we have $a_0+b_0+(-c_0)+(-d_0) = 4$ and then $a_i+b_i+c_i+d_i = \pm 2 + 2(c_i+d_i) = \pm 2$. □

Corollary 1. *If in Theorem 2 we have (ii)'* $a_0+b_0+c_0+d_0=\pm 2$ *instead of (ii), then*

$$(x_0+y_0+z_0+w_0)-(a_0+b_0+c_0+d_0)\equiv 0\ (mod\ 8),$$
$$x_j+y_j+z_j+w_j\equiv 0\ (\mathrm{mod}\ 4),\quad j=1,2,\ldots,\tfrac{1}{2}(p-1).$$

Proof. If we consider A, B, C, $-D$, then

$$a_0+b_0+c_0+(-d_0)=a_0+b_0+c_0+d_0-2d_0=0,\pm 4,$$

then Williamson's result holds, i.e.,

$$a_i+b_i+c_i+(-d_i)=\pm 2 \quad \text{or} \quad a_i+b_i+c_i+d_i=0,\pm 4.$$

So

$$(x_0+y_0+z_0+w_0)-(a_0+b_0+c_0+d_0)\equiv 0\ (\mathrm{mod}\ 8)$$

and

$$x_j+y_j+z_j+w_j=\sum_{\substack{i\equiv j\ (\mathrm{mod}\ p)\\ i<m}}(a_i+b_i+c_i+d_i)\equiv 0\ (\mathrm{mod}\ 4),$$
$$j=1,2,\ldots,\tfrac{1}{2}(p-1).\quad \square$$

Now for a given decomposition

$$a^2+b^2+c^2+d^2=4m$$

we can take a, b, c, d to be positive and so a_0, b_0, c_0, d_0 are uniquely determined.

In our algorithm given in Section 5 we first find all sequences $X_p=(x_0,\ldots,x_{p-1})$ such that

$$-q\leqslant x_j\leqslant q,\quad j=0,1,2,\ldots,p-1,$$
$$x_j=x_{p-j},\qquad x_j \text{ odd},\quad j=1,2,\ldots,\tfrac{1}{2}(p-1),$$
$$\sum_{j=0}^{p-1}x_j=a.$$

similarly we construct all sequences

$$Y_p=(y_0,y_1,\ldots,y_{p-1}),\qquad Z_p=(z_0,z_1,\ldots,z_{p-1}),\qquad W_p=(w_0,w_1,\ldots,w_{p-1}).$$

Then examine which quadruples X_p, Y_p, Z_p, W_p satisfy also (3). However it is computationally faster to examine first if for a given quadruple X_p, Y_p, Z_p, W_p the relations in Theorem 2(ii) hold when

$$a_0+b_0+c_0+d_0=0,\pm 4$$

(or of Corollary 1 when $a_0+b_0+c_0+d_0=\pm 2$). These quadruples are then examined whether they satisfy (3).

3. An example

For $m = 15 = 3 \cdot 5$ and for the decomposition $60 = 7^2 + 3^2 + 1^2 + 1^2$ all X_3, Y_3, Z_3, W_3 satisfying (2) are:

$$X_3 = (5, 1, 1) \quad \text{or} \quad (1, 3, 3) \quad \text{or} \quad (-3, 5, 5),$$
$$Y_3 = (5, -1, -1) \quad \text{or} \quad (1, 1, 1) \quad \text{or} \quad (-3, 3, 3),$$
$$Z_3 = (3, -1, -1) \quad \text{or} \quad (-1, 1, 1) \quad \text{or} \quad (-5, 3, 3),$$
$$W_3 = (3, -1, -1) \quad \text{or} \quad (-1, 1, 1) \quad \text{or} \quad (-5, 3, 3).$$

It is easy to see that there are 6 solutions satisfying (3) (given in Table 1).

At this point we can construct the possible quadruples A, B, C, D. To do this take for example solution (1) of Table 1 and note that:

(i) $\binom{5}{2} = 10$ different A's giving $X_3 = (5, 1, 1)$,

(ii) 10 different B's giving $Y_3 = (5, -1, -1)$,

(iii) $20 = 2 \cdot 10$ different C's giving $Z_3 = (-1, 1, 1)$,

(iv) $20 = 2 \cdot 10$ different D's giving $W_3 = (-1, 1, 1)$.

A, B, C, D are 15×15 circulant and symmetric $(+1, -1)$ matrices. Hence to the solution: $X_3 = (5, 1, 1)$, $Y_3 = (5, -1, -1)$, $Z_3 = (-1, 1, 1)$, $W_3 = (-1, 1, 1)$ correspond $10 \cdot 10 \cdot 20 \cdot 20 = 40\,000$ quadruples A, B, C, D which have to be examined whether they satisfy (1).

To the six solutions X_3, Y_3, Z_3, W_3 given in Table 1, correspond 120 000 possible quadruples A, B, C, D. Without our method we would have to examine $\binom{7}{2}$ possible A's, $\binom{7}{3}$ possible B's, C's, D's, i.e., in all $\binom{7}{2} \cdot \binom{7}{3}^3 = 900\,375$ quadruples A, B, C, D for the above decomposition $60 = 7^2 + 3^2 + 1^2 + 1^2$.

If $p \neq q$ we do not need to find explicitly all 120 000 quadruples A, B, C, D mentioned above but proceed to the next two steps which give another reduction in computational time:

I) Find similarly all solutions for X_5, Y_5, Z_5, W_5 satisfying (2) and (3). We easily see that there are 8 solutions given in Table 2. If we take for example solution (5), of Table 2, i.e.,

$$X_5 = (3, -1, 3, 3, -1), \qquad Y_5 = (-1, -1, 3, 3, -1),$$
$$Z_5 = (1, -1, 1, 1, -1), \qquad W_5 = (1, 1, -1, -1, 1).$$

Table 1. Quadruples X_3, Y_3, Z_3, W_3 satisfying (2) and (3)

	X_3	Y_3	Z_3	W_3
1)	(5, 1, 1)	(5, −1, −1)	(−1, 1, 1)	(−1, 1, 1)
2)	(5, 1, 1)	(−3, 3, 3)	(−1, 1, 1)	(−1, 1, 1)
3)	(1, 3, 3)	(5, −1, −1)	(3, −1, −1)	(−1, 1, 1)
4)	(1, 3, 3)	(−3, 3, 3)	(3, −1, −1)	(−1, 1, 1)
5)	(1, 3, 3)	(5, −1, −1)	(−1, 1, 1)	(3, −1, −1)
6)	(1, 3, 3)	(−3, 3, 3)	(−1, 1, 1)	(3, −1, −1)

Table 2. Quadruples X_5, Y_5, Z_5, W_5 satisfying (2) and (3)

	X_5	Y_5	Z_5	W_5
1)	(−1, 1, 3, 3, 1)	(−1, 3, −1, −1, 3)	(−3, 1, 1, 1, 1)	(1, 1, −1, −1, 1)
2)	(−1, 1, 3, 3, 1)	(3, −1, 1, 1, −1)	(−3, 1, 1, 1, 1)	(−3, 1, 1, 1, 1)
3)	(−1, 3, 1, 1, 3)	(−1, −1, 3, 3, −1)	(−3, 1, 1, 1, 1)	(1, −1, 1, 1, −1)
4)	(−1, 3, 1, 1, 3)	(3, 1, −1, −1, 1)	(−3, 1, 1, 1, 1)	(−3, 1, 1, 1, 1)
5)	(3, −1, 3, 3, −1)	(−1, −1, 3, 3, −1)	(1, −1, 1, 1, −1)	(1, 1, −1, −1, 1)
6)	(3, −1, 3, 3, −1)	(3, 1, −1, −1, 1)	(−3, 1, 1, 1, 1)	(1, 1, −1, −1, 1)
7)	(3, 3, −1, −1, 3)	(−1, 3, −1, −1, 3)	(1, −1, 1, 1, −1)	(1, 1, −1, −1, 1)
8)	(3, 3, −1, −1, 3)	(3, −1, 1, 1, −1)	(−3, 1, 1, 1, 1)	(1, −1, 1, 1, −1)

It is easy to verify that there are

(i) 3 A's giving X_5,

(ii) 3 B's giving Y_5,

(iii) 9 C's giving Z_5,

(iv) 9 D's giving W_5,

in all there are $3 \cdot 3 \cdot 9 \cdot 9 = 729$ quadruples A, B, C, D corresponding to solution (5) which have to be examined whether they satisfy (1).

II) Combine each solution X_3, Y_3, Z_3, W_3 with every solution X_5, Y_5, Z_5, W_5. For example take the solutions

$$X_3 = (5, 1, 1), \quad Y_3 = (5, -1, -1), \quad Z_3 = (-1, 1, 1), \quad W_3 = (-1, 1, 1),$$

and

$$X_5 = (3, -1, 3, 3, -1), \quad Y_5 = (-1, -1, 3, 3, -1),$$
$$Z_5 = (1, -1, 1, 1, -1), \quad W_5 = (1, 1, -1, -1, 1).$$

By inspection we see that:

(i) Out of the 3 A's giving X_5 there is only one A giving also X_3, i.e., $A = (+-++-++++++-++-)$.

(ii) Out of the 3 B's giving Y_5 there is only one B giving also Y_3, i.e., $B = (+-++--++++--++-)$.

(iii) Out of the 9 C's giving Z_5 there are 5 giving also Z_3, i.e.,

$C = (-+-+-+-++-+-+-+)$ or $(---+++-++-+++--)$ or
$(--+--++++++--+-)$ or $(-+++-+----+-+++)$ or
$(--++++----++++-)$.

(iv) Out of the 9 D's giving W_5 there are 5 giving also W_3, i.e.,

$D = (--+-+++--++++-+-)$ or $(----++++++++---)$ or
$(-++--++--++--++)$ or $(-+---++++++---+)$ or
$(-+-+++----+++-+)$.

Hence there are $1 \cdot 1 \cdot 5 \cdot 5 = 25$ quadruples of A, B, C, D corresponding to the above pair of solutions X_3, Y_3, Z_3, W_3 and X_5, Y_5, Z_5, W_5.

These 25 quadruples have to be examined whether they satisfy (1), this may be done by hand and there is only one such quadruple, i.e.,

$$A = (+-++-+++++++-++-), \qquad B = (+-++--+++++--++-),$$
$$C = (--+--++++++--+-), \qquad D = (-+-+++----+++-+),$$

with $A^2 + B^2 + C^2 + D^2 = 60I_{15}$, where + stands for 1 and − for −1.

In the same way we examine every one of the $6 \cdot 8 = 48$ pairs of solutions (X_3, Y_3, Z_3, W_3) and (X_5, Y_5, Z_5, W_5). The next stage is to take the decomposition $60 = 5^2 + 5^2 + 3^2 + 1^2$ and repeat the same procedure as before.

Another serious reduction of the computational time is achieved if we consider only non-equivalent quadruples, i.e., if we apply the transformation $j \to j \cdot s \pmod m$, where $(s, m) = 1$, then $a_j \to a_{j \cdot s}$, $b_j \to b_{j \cdot s}$, $c_j \to c_{j \cdot s}$, $d_j \to d_{j \cdot s}$, $j = 0, 1, 2, \ldots, m-1$ and the transformed A, B, C, D remain circulant and symmetric.

Note that j and $m - j$ give identical quadruples because of the symmetry of A, B, C, D.

We need only to know one quadruple in every equivalent class.

For $m = 15$ there are at most 4 equivalent quadruples in each equivalent class ($j = 1, 2, 4, 7$).

Now the transformation $j \to j \cdot s \pmod m$, $(s, m) = 1$, because of (2) transforms equivalent classes of A, B, C, D into equivalent classes of X_p, Y_p, Z_p, W_p and X_q, Y_q, Z_q, W_q with corresponding transformations

$$j \to j \cdot s \pmod p, \quad (s, m) = 1, s < p \quad \text{and}$$
$$j \to j \cdot s \pmod q, \quad (s, m) = 1, s < q.$$

(From $j \to j \cdot s \pmod p$ and $j \to j(p - s) \pmod p$ apply only one, because they give identical transformations due to the symmetry of X_p, Y_p, Z_p, W_p, similarly for $j \to j \cdot s \pmod q$ and $j \to j(q - s) \pmod q$).

Knowing (X_p, Y_p, Z_p, W_p) and (X_q, Y_q, Z_q, W_q) we can find their equivalent classes.

Attention is needed here because to a representative of a class A, B, C, D we do not know which is the pair of representatives of the corresponding classes of X_p, Y_p, Z_p, W_p and X_q, Y_q, Z_q, W_q.

However, if we consider one representative from each class of X_q, Y_q, Z_q, W_q $(q > p)$ and combine it with all solutions (equivalent or not) of X_p, Y_p, Z_p, W_p then all non-equivalent, A, B, C, D will be found.

From $m = 15$, $p = 3$, $q = 5$ then the 8 solutions X_5, Y_5, Z_5, W_5 of Table 2 reduce to the 4 non-equivalent solutions ($s = 2$): (1), (2), (5), (6) of Table 2.

Hence instead of $6 \cdot 8 = 48$ pairs of solutions X_3, Y_3, Z_3, W_3 and X_5, Y_5, Z_5, W_5 we only examine $6 \cdot 4 = 24$ such pairs or $24 \cdot 25 = 600$ quadruples A, B, C, D approximately.

Originally, without our method, for the decomposition $60 = 7^2 + 3^2 + 1^2 + 1^2$,

there were 900 375 quadruples to be examined whether they satisfy (1) or at least $900\,375:4 \approx 225\,094$ non-equivalent quadruples (here $j = 2, 4, 7$ and there are at most 4 equivalent not identical quadruples in each equivalent class).

In conclusion our computational time is approximately $600:225\,094 \approx 0.0027$ of the original time.

4. The case $m = 33 = 3 \cdot 11$

(i) For $132 = 11^2 + 3^2 + 1^2 + 1^2$ we found 12 solutions for $p = 3$ and 83 non-equivalent solutions for $q = 11$. So we examined $12 \cdot 83 = 996$ pairs of solutions which gave no solution for A, B, C, D, i.e., no Hadamard matrices exist of the Williamson type (circulant and symmetric) with the above decomposition of 132.

(ii) For $132 = 9^2 + 7^2 + 1^2 + 1^2$ we found 12 solutions for $p = 3$ and 81 non-equivalent solutions for $q = 11$. Out of the $12 \cdot 81 = 972$ pairs of solutions only the pair

$$X_3 = (7, 1, 1), \qquad \hat{X}_{11} = (3, -1, 1, 1, 1, 1, 1, 1, 1, 1, -1),$$
$$Y_3 = (5, 1, 1), \qquad \hat{Y}_{11} = (-3, 1, 3, -1, 1, 1, 1, 1, -1, 3, 1),$$
$$Z_3 = (3, -1, -1), \qquad \hat{Z}_{11} = (-1, -1, 1, 3, -1, -1, -1, -1, 3, 1, -1),$$
$$W_3 = (-5, 3, 3), \qquad \hat{W}_{11} = (3, 1, 3, -3, -1, -1, -1, -1, -3, 3, 1),$$

gave one solutions for A, B, C, D up to equivalence.

(iii) For $132 = 9^2 + 5^2 + 5^2 + 1^2$ we found 12 solutions for $p = 3$ and 97 non-equivalent solutions for $q = 11$. Out of the $12 \cdot 97 = 1164$ pairs of solutions only the two pairs

(a)
$$X_3 = (7, 1, 1), \qquad \hat{X}_{11} = (3, -1, -1, 1, 3, 1, 1, 3, 1, -1, -1),$$
$$Y_3 = (7, -1, -1), \qquad \hat{Y}_{11} = (3, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1),$$
$$Z_3 = (-1, 3, 3), \qquad \hat{Z}_{11} = (3, 3, -1, 1, -3, 1, 1, -3, 1, -1, 3,),$$
$$W_3 = (3, -1, -1), \qquad \hat{W}_{11} = (-1, 1, -1, -1, -1, 3, 3, -1, -1, -1, 1),$$

and

(b)
$$X_3 = (3, 3, 3), \qquad \hat{X}_{11} = (3, -1, -1, 3, 1, 1, 1, 1, 3, -1, -1),$$
$$Y_3 = (-5, 5, 5), \qquad \hat{Y}_{11} = (3, 1, 1, -1, -1, 1, 1, -1, -1, 1, 1),$$
$$Z_3 = (-1, 3, 3), \qquad \hat{Z}_{11} = (3, 3, -3, 1, -1, 1, 1, -1, 1, -3, 3),$$
$$W_3 = (3, -1, -1), \qquad \hat{W}_{11} = (-1, 3, 1, -1, -1, -1, -1, -1, -1, 1, 3),$$

gave two non-equivalent solutions for A, B, C, D.

(iv) For $132 = 7^2 + 7^2 + 5^2 + 3^2$ we found 12 solutions for $p = 3$ and 103 non-

equivalent solutions for $q=11$. Out of $12 \cdot 103 = 1236$ pairs of solutions only the pair

$$X_3 = (-3, 5, 5), \qquad \hat{X}_{11} = (1, -1, 1, -1, 3, 1, 1, 3, -1, 1, -1),$$
$$Y_3 = (5, 1, 1) \qquad \hat{Y}_{11} = (-3, 1, -1, 3, 3, -1, -1, 3, 3, -1, 1),$$
$$Z_3 = (-1, 3, 3) \qquad \hat{Z}_{11} = (3, 3, -1, -1, 1, -1, -1, 1, -1, -1, 3),$$
$$W_3 = (5, -1, -1), \qquad \hat{W}_{11} = (-3, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1),$$

gave one solution for A, B, C, D up to equivalence.

This means that there are in all four non-equivalent Hadamard matrices of the Williamson type of order $132 = 4 \cdot 33$.

5. The Algorithm

For a given decomposition $4m = a^2 + b^2 + c^2 + d^2$, with $m = p \cdot q$, $p < q$, our algorithm consists of four stages:

I) 1. Form all sequences $X_p = (x_0, x_1, \ldots, x_{p-1})$ satisfying

$$\text{(i)} \sum_{i=0}^{p-1} x_i = a, \quad \text{(ii)} \ -q \leqslant x_i \leqslant q, \quad \text{(iii)} \ x_i \text{ odd},$$

$$\text{(iv)} \ x_i = x_{p-i}, \quad i = 1, 2, \ldots, \tfrac{1}{2}(p-1).$$

2. Repeat the construction for Y_p, Z_p, W_p replacing a with b, c, d respectively.
3. Examine which quadruples X_p, Y_p, Z_p, W_p satisfy

$$X_p^2 + Y_p^2 + Z_p^2 + W_p^2 = 4mI_p.$$

II) 1. Repeat stage I interchanging p and q.
2. Find all non-equivalent solutions by applying the transformation $j \to j \cdot s \pmod q$ to each solution X_q, Y_q, Z_q, W_q, where $(s, m) = 1$ for every $s < q$. (From $j \to j \cdot s \pmod q$ and $j \to j(q-s) \pmod q$ apply only one).

III) 1. If there are h_1 solutions X_p, Y_p, Z_p, W_p and h_2 non-equivalent solutions $\hat{X}_q$, $\hat{Y}_q$, $\hat{Z}_q$, $\hat{W}_q$, form the $h_1 \cdot h_2$ combined solutions X_p, Y_p, Z_p, W_p, $\hat{X}_q$, $\hat{Y}_q$, $\hat{Z}_q$, $\hat{W}_q$.
2. Find $A = (a_0, a_1, \ldots, a_{m-1})$ from:

$$a_i = a_{m-i}, \quad i = 1, 2, \ldots, \tfrac{1}{2}(m-1),$$

$$\sum_{\substack{i \equiv j \pmod p \\ i < m}} a_i = x_j, \quad j = 0, 1, 2, \ldots, \tfrac{1}{2}(p-1),$$

$$\sum_{\substack{i \equiv j \pmod q \\ i < m}} a_i = \hat{x}_j, \quad j = 0, 1, 2, \ldots, \tfrac{1}{2}(q-1),$$

where $X_p = (x_0, x_1, \ldots, x_{p-1})$, $\hat{X}_q = (\hat{x}_0, \hat{x}_1, \ldots, \hat{x}_{q-1})$.

3. Find B, C, D similarly

IV) Examine which quadruples A, B, C, D satisfy $A^2+B^2+C^2+D^2=4mI_m$. Now repeat stages, I, II, III, IV for every decomposition of $4m$ as the sum of four odd squares.

If $p=q$ then the algorithm is:

1) 1. Perform steps 1, 2, 3 of stage I of the previous algorithm

2. Find all non-equivalent solutions by applying the transformation $j\to j\cdot s \pmod p$ to each solution X_p, Y_p, Z_p, W_p, where $(s,m)=1$ for every $s<p$ (From $j\to j\cdot s \pmod p$ and $j\to j(p-s) \pmod p$ apply only one).

2) 1. Find $A=(a_0, a_1, \ldots, a_{m-1})$ from:

$$a_i = a_{m-i}, \qquad i=1,2,\ldots,\tfrac{1}{2}(m-1),$$

$$\sum_{\substack{i\equiv j \pmod p \\ i<m}} a_i = x_j, \quad j=0,1,2,\ldots,\tfrac{1}{2}(p-1),$$

where $X_p=(x_0, x_1, \ldots, x_{p-1})$.

2. Find B, C, D similarly.

3) Examine which quadruples A, B, C, D satisfy $A^2+B^2+C^2+D^2=4mI_m$.

Now repeat stages 1, 2, 3 for every decomposition of $4m$ as the sum of four odd squares.

Appendix

Here we give the four non-equivalent Hadamard matrices of the Williamson type of order 132 using the array of Williamson:

$$H=\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix},$$

where A, B, C, D are circulant and symmetric matrices of order $m=33$.

(i) $132=11^2+3^2+1^2+1^2$, no solution exists.

(ii) $132=9^2+7^2+1^2+1^2$,

$A=(+--+++---+-++++++++++++-+---+++--)$,

$B=(--+-+++-+++-++-+--+-++-+++-+++-+-)$,

$C=(++-++-+-++---++----++---++-+-++-+)$,

$D=(+++-+----+++-+--++--+-+++----+-++)$.

(iii) $132=9^2+5^2+5^2+1^2$,

(a)

$A=(+--++-++++++-+--+++---++++++-++--)$,

$B=(+-++++-++-++-----------++-++-++++-)$,

$C=(++-+-+--+-++++--++--++++-+--+-+-+)$,

$D=(+---+++--++-+-+-++-+-+-++--+++---)$;

(b)

$A = (+--+++--+--++++++++++++--+--++++--),$

$B = (+++++++----++-+--++--+-++----++++),$

$C = (++-+-+-+-+--+++-+-++-+-+++--+-+-+-+),$

$D = (++--+-+--++-+++----+++-++--+-+--+).$

(iv) $132 = 7^2 + 7^2 + 5^2 + 3^2,$

$A = (--++++-+--++-+-++++-+-++--+-++++-),$

$B = (-+-++-++++++--++--++---++++-++-+),$

$C = (+++-++----++-++--++-+++----++-++),$

$D = (----+-+-+++-++-++++-++-+++-+-+---),$

where + stands for 1 and − for −1.

References

[1] S.S. Agayan and A.G. Sarukhanyan, Recurrence formulas for the construction of Williamson-type matrices, Math. Notes 30 (1982) 796–804.

[2] L.D. Baumert, Hadamard matrices of orders 116 and 232, Bull. Amer. Math. Soc. 72 (1966) 237.

[3] L.D. Baumert, S.W. Golomb and M. Hall Jr, Discovery of an Hadamard matrix of order 92, Bull. Amer. Math. Soc. 68 (1962) 237–238.

[4] L.D. Baumert and M. Hall Jr, Hadamard Matrices of the Williamson Type, Math. Comp. 19 (1965) 442–447.

[5] M. Hall Jr., Combinatorial Theory (Blaisdell, Waltham, MA, 1967).

[6] A. Hedayat and W.D. Wallis, Hadamard matrices and their applications, Ann. Statist. 6(6) (1978) 1184–1238.

[7] A.N. Geramita and J. Seberry, Orthogonal Designs (Dekker, New York, 1979).

[8] K. Sawade, Hadamard matrices of order 100 and 108, Bull. Nagoya Inst. Technol. 29 (1977) 147–153.

[9] J. Seberry Wallis, Construction of Williamson type matrices, Linear and Multilinear Algebra 3 (1975) 197–207.

[10] J. Seberry Wallis, On Hadamard matrices, J. Combin. Theory Ser. A 18 (1975) 149–164.

[11] R.J. Turyn, An infinite class of Williamson matrices, J. Combin. Theory Ser. A 12 (1972) 319–321.

[12] W.D. Wallis, A.P. Street and J. Seberry Wallis, Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices, Lecture Notes in Math. Vol 292 (Springer, Berlin, 1972).

[13] A.L. Whiteman, An infinite family of Hadamard matrices of Williamson type, J. Combin. Theory Ser. A 14 (1973) 334–340.

[14] J. Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Math. J. 11 (1944) 65–81.

[15] M. Yamada, On the Williamson type j matrices of orders $4 \cdot 29$, $4 \cdot 41$ and $4 \cdot 37$, J. Combin. Theory Ser. A 27 (1979) 378–381.